EMBO reports

science & society

Facing the future of biometrics

Demand for safety and security in the public and private sectors is driving research in this rapidly growing field

Christoph Busch

For more than a century, criminal investigators have used fingerprints to identify suspects on the basis of evidence left at the crime scene. Whereas fingerprints were once compared visually, today computers speed up the process: the Automated Fingerprint Identification System (AFIS), now used in most Western countries, compares traces found at a crime scene with millions of stored fingerprint images in just a few seconds. Recently, the police in various German cities introduced mobile AFIS, enabling comparisons to be made immediately over mobile communication networks. However, it is not only criminal investigators who use such technology; many commercial access-control systems use identification systems based on biometrics—the automated recognition of individuals by using behavioural and/or biological characteristics. An increasing demand for safety and security in both the public and private sectors is now driving research in this rapidly growing field.

In addition to fingerprints, biometric technologies can make use of a rich variety of anatomical characteristics, such as images of the face, iris or retina, or representations of the geometry of the hand. These systems also use behavioural or physiological characteristics, such as a written signature, voice or the typing pattern on a keyboard. Such functions

> …[the] new national ID cards will not only be more secure travel documents—such as the ePass—but will also support new applications that are based on electronic signatures

create an individual signal that can be measured by biometric technology.

Anyone who has recently travelled to the USA is familiar with the procedure: at US border control, the prints of both index fingers are taken, as is a digital portrait photo. This additional security measure is used not only to combat terrorism but also to monitor residence permits. From the perspective of its operators, it has been a success—after its implementation in 2004, it took only a few months of operation for the system to spot several hundred travellers who wanted to enter the USA while being on a watch list.

Biometrics is also important for the planned 'ePass' for citizens of the European Union (EU). The EU Council Regulation on standards for security features and biometrics in EU citizens' passports defined the timeline for introducing digital face and fingerprint images in all European passports issued after October 2006 (Council of the European Union, 2004). This regulation will implement the technical specifications established by the International Civil Aviation Organization (ICAO; Montreal, Canada) in all EU member states (ICAO, 2004). The expansion of biometric data is intended to increase security and to reduce the processing time at borders. Although a photo has been an integral part of passports for the past few decades, the images in every German passport issued after October 2005 are now stored electronically. From March 2007, passports issued in EU member states will also include electronic fingerprint images. As soon as a larger percentage of EU citizens are equipped with this new ePass, it will certainly increase the use of biometrics at border controls in the EU and other countries.

> After all, humans have evolved their own biometric procedures to look at and recognize the faces of other humans and react accordingly

Although European standardization bodies have recently agreed on a format for the European Citizen Card it is still unclear what national implementations will look like (European Committee for Standardization, 2005). If the EU member states adopt this standard, their new national ID cards will not only be more secure travel documents—such as the ePass—but will also support new applications that are based on electronic signatures. The plan is to incorporate a radiofrequency identification chip in addition to biometric data and to establish a high level of interoperability with electronic passports. However, national identity cards, such as the planned eID in Germany, may serve both governmental and commercial needs by allowing its users to access e-government, e-banking or e-commerce systems. In e-banking in particular, there is a demand for reliable authentication methods for system operators and customers. The vulnerability of online systems is highlighted by an increasing number of 'phishing' attacks—e-mails purportedly from a bank, asking for the user's financial information and account password—and other attempts to hijack the connection between an online bank and its customers. As banks are unlikely to close down their online services, the only way to solve this pressing security problem is to reduce the possibility of fraud by using more secure access control mechanisms.

To authenticate a person, personal features are measured and compared with reference data stored either in a document—such as a passport—or in a database. The aim of this comparison is to determine whether the biometric characteristics of that person match the previously recorded representation in the reference data. Biometric systems can therefore work as either verification or identification systems. In the case of identification, the identity of a person is usually determined by matching his or her features against a database, whereas the purpose of verification is to confirm a person's claimed identity against data stored in a passport or other document.

The biometric recognition process involves three steps: acquisition, feature extraction and comparison. First, biometric characteristics are acquired through measurements. A sensor, such as a camera, microphone or fingerprint scanner, captures the specific characteristics of a subject and creates a digital representation, thus defined as the biometric sample: a photograph, a voice recording or a scanned fingerprint, for example.

Feature extraction is a mathematical transformation that extracts distinguishing and reproducible data from the sample. These data are a concise representation of the original information and are defined as biometric features. A template—a set of these features—is compared directly with biometric features from other samples. The so-called enrolment process stores one or more biometric samples or templates in a database or in a secure travel document and attributes them to a subject. This reference data can then be used for comparison in future identification or verification processes.

> Even the low-quality image from a mobile phone camera is sufficient to successfully present 'biometric characteristics' to a face-recognition system

The last step is to compare an individual's biometric characteristics against the biometric references of one or more individuals. This process produces a score that indicates the similarity (a value close to, but rarely, one) or dissimilarity (a value close to zero) of two samples. Only by comparison can the recognition system decide if a presented sample matches a stored reference. This principle of biometric recognition is the same in all systems regardless of their particular technology or the features measured: a biometric system must 'learn' about the biometric characteristics of the subject before it can 'recognize' a person.

Facial recognition in particular has an important role in the development of reliable and easy-to-use biometric identification and verification systems. It is certainly the least intrusive method and is an obvious way to identify a person. After all, humans have evolved their own biometric procedures to look at and recognize the faces of other humans and react accordingly. However, whereas the human visual system intuitively collects, analyses and integrates additional information—such as body shape and size—in the decision process, a computer-based system has neither the capabilities nor the sophistication of the human brain.

So far, facial recognition systems have depended on a conventional camera to capture two-dimensional (2D), frontal pictures. After the acquisition, the system analyses the image by first concentrating on the area in which the face of the subject is located. The next step locates the face very precisely using unique facial

landmarks to fine-tune the recognition process. These are typically significant areas, such as the corners of the eyes, mouth, nose or chin, which can be identified not only visually by human inspection but also through an automated biometric system. The next step is to extract this information from the image—a difficult task, which requires that the image was taken under controlled conditions. A different hairstyle, natural ageing, a beard or new glasses creates strong variations in the computed features and therefore makes identification more difficult.

Furthermore, the quality of the image must be extremely high for 2D face recognition. Certain criteria, such as a high resolution, a full-frontal perspective, sufficient contrast and good lighting, must be fulfilled. Other acquisition conditions are also required, such as a neutral facial expression and the removal of any glasses, headgear or hair that obscures facial landmarks. Without these requirements, the biometric system may recognize the person very slowly or not at all (Funk *et al*, 2005). In any case, it is very rare that the perspective and expression of the face in the presented sample are identical to the reference image. As a result of this sensitivity, 2D face recognition has been unsatisfactory.

> The main advantage of biometric authentication is that it reduces the risk of information (passwords) or tokens (keys or chip cards) being stolen or passed on to unauthorized people…

Consequently, 2D face recognition systems are currently unable to provide a reliable mechanism for live detection to protect against identity theft. As many science fiction and action films have shown, such access control sensors can be easily fooled by presenting a photo to the camera or rendering a video of the person on a laptop. Even the low-quality image from a mobile phone camera is sufficient to present 'biometric characteristics' successfully to a face-recognition system. There are too few systems available to perform live detection and thus prevent an identity being faked by simply presenting a still image. As a result, this technology is unreliable without additional supervision by a human operator.

A more sophisticated and promising approach is three-dimensional (3D) face recognition—now a popular research area in academic and industrial laboratories, as it offers far greater reliability (Chang *et al*, 2005). Compared with a 2D image, a 3D model can be used to identify a person much more easily, even if the head is tilted or if the camera is not perfectly aligned with the subject. Although this method also relies on detecting facial landmarks, such systems can create a much more reliable set of biometric features using the third dimension. In fact, facial landmarks are used to align the probe to the orientation of the reference model and only then, if the orientation is identical or close to identical, are similarity measurements made. The measurements themselves can be based on local colour or texture analysis, but also on measurements derived from the third dimension, such as local flexions or distances between geometric surfaces.

Depth information can be recorded using a lighting system that projects coloured stripes or patterns on the subject's face to provide a complete facial geometry. One key advantage of 3D images is that, unlike two-dimensional images, geometric surfaces are metrically correct. Basic measurements—the 'soft' biometric characteristics—such as the distance between the eyes, are not lost during the conversion to normalized formats. Furthermore, as 3D face acquisition collects far more distinguishing information than its 2D counterpart, the level of detail of the classification procedure, and therefore the biometric performance of such systems, is improved. Consequently, it is difficult to fool a 3D facial recognition system. First, it is laborious to capture the face geometry of an authorized person without their cooperation. Second, it is costly and time-consuming to produce a print-out of the model, which could easily be detected in a simple live check. However, 3D face recognition systems are still in the early research stages.

The main advantage of biometric authentication is that it reduces the risk of information (passwords) or tokens (keys or chip cards) being stolen or passed on to unauthorized people, intentionally or unintentionally. It is also a user-friendly technology, as customers no longer need to remember a personal identification number or carry cards or documents with them. Unlike knowledge-based or possession-based procedures, the biometric characteristics of an individual are an integral part of a person and usually last for a long time.

In the future, we will increasingly see biometric systems for both identification and verification. In addition to the ICAO recommendations, a wide range of non-government applications exist. Biometric systems will enable access to secure or sensitive areas, such as energy supply facilities, nuclear power stations or emergency service control centres. Furthermore, a digital citizen card also opens up new opportunities for logical access controls, for example in e-government, e-banking or e-business. Public demand for these applications may be the driving force behind further progress in biometrics research.

REFERENCES

Council of the European Union (2004) Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. Brussels, Belgium: Council of the European Union

Chang KI, Bowyer KW, Flynn PJ (2005) An evaluation of multimodal 2D+3D face biometrics. *IEEE Trans Pattern Anal Mach Intell* **27:** 619–624

European Committee for Standardization (2005) Identification card systems—European Citizen Card—Part 2: Logical data structures and card services. Brussels, Belgium: European Committee for Standardization

Funk W, Arnold M, Busch C, Munde A (2005) Evaluation of image compression algorithms for fingerprint and face recognition systems. In: *Systems, Man and Cybernetics (SMC) Information Assurance Workshop. Proceedings from the Sixth Annual IEEE*, pp 72–78. West Point, NY, USA: IEEE Computer Society

ICAO (2004) Biometrics Deployment of Machine Readable Travel Documents. Version 2.0. Montreal, Canada: International Civil Aviation Organization

Christoph Busch is at the Fraunhofer Institute for Computer Graphics and the University of Applied Science in Darmstadt, Germany.
E-mail: christoph.busch@igd.fraunhofer.de

doi:10.1038/sj.embor.7400723